# Information Support Plan (ISP

OASD(NII)/DCIO

Paul Szabados
paul.szabados@osd.mil
(703) 607-0246

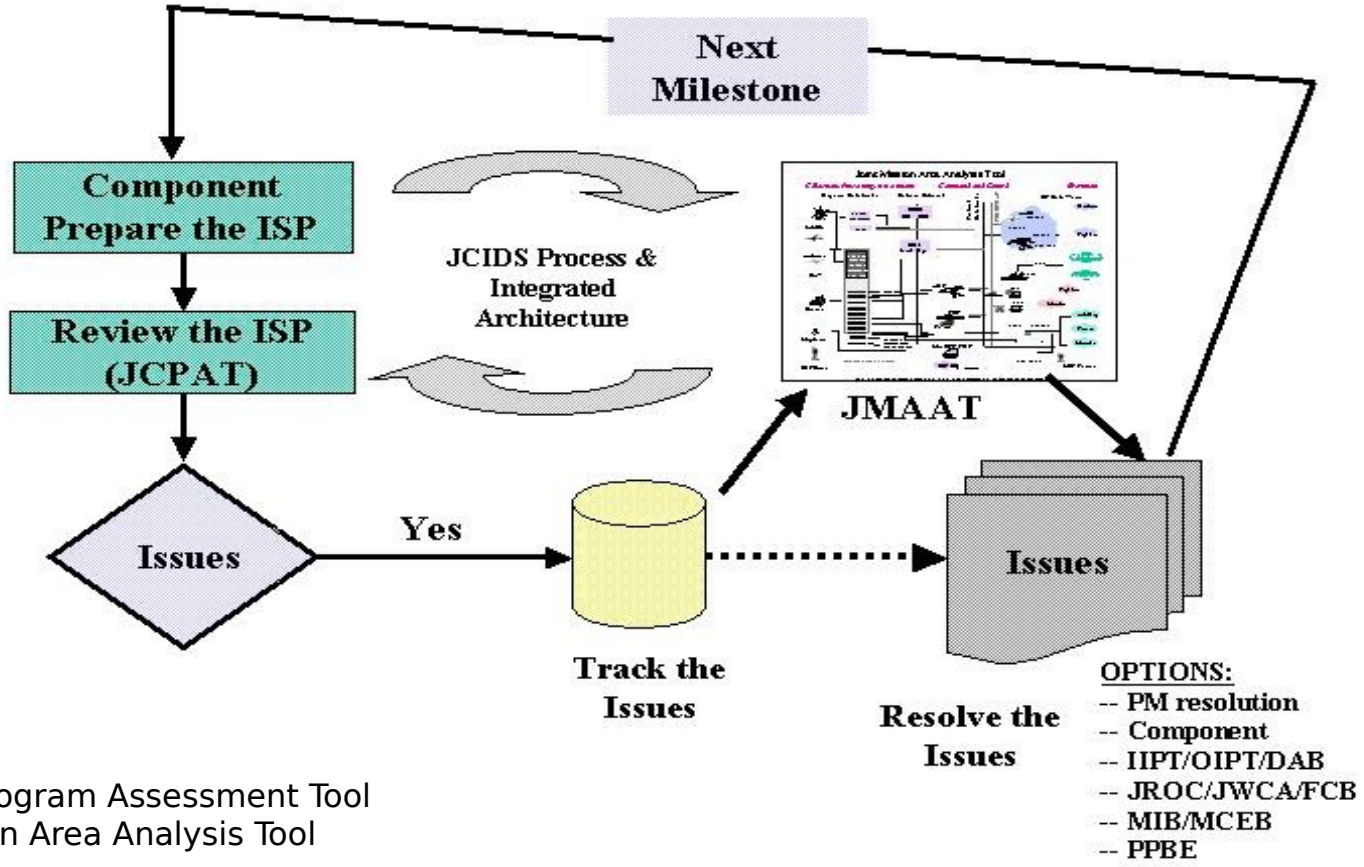
# Briefing Overview

- ISP Executive-Level Brief
- ISP Pilot Program (26 August 2005)
- ISP Enhancement Project (Summer 200
- ISP References and POCs

# Value

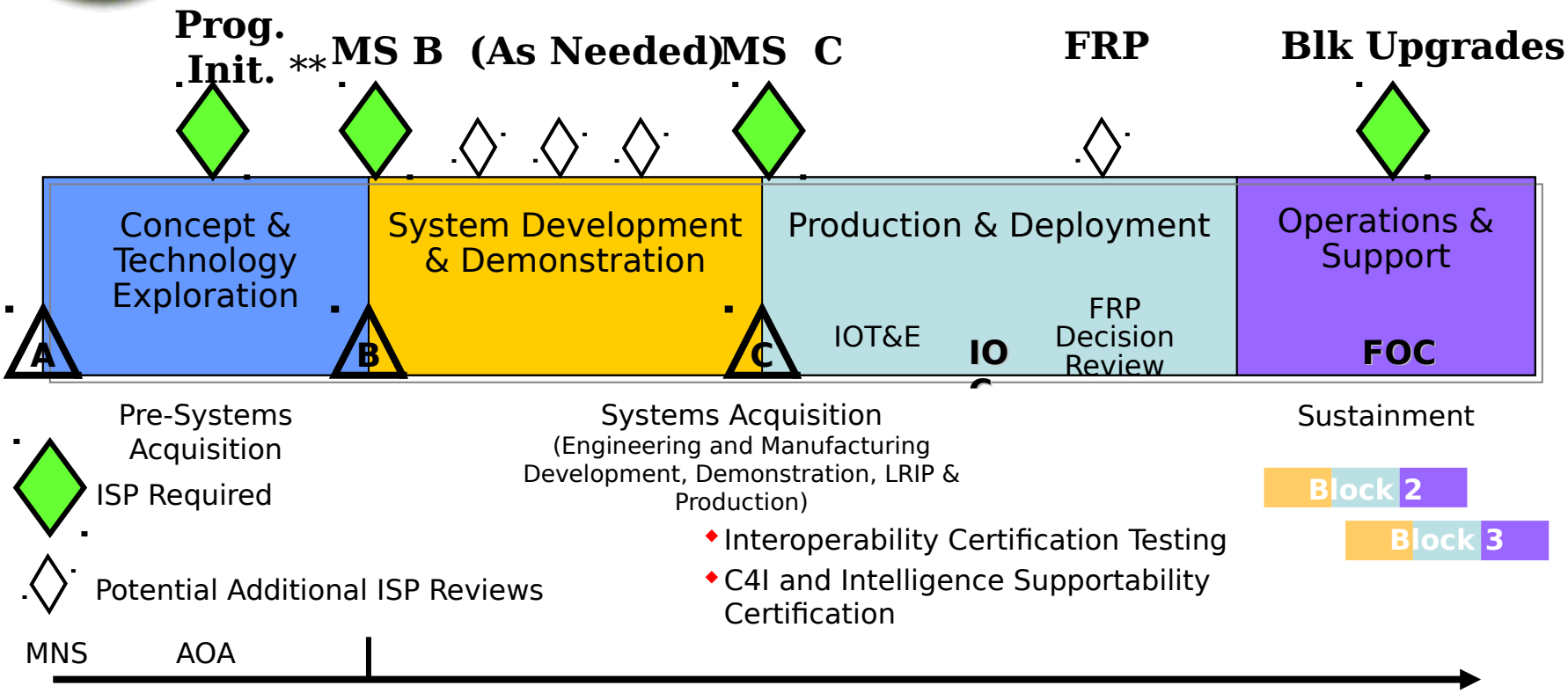
- Documents transformation toward net-centricity and DoD CIO goals
- Provides for a rigorous IT needs and supportability analysis preventing gaps and lack of capabilities
- Provides evidence and over-sight of system engineering
- Collects DoD information issues
- Provides a resource for cross-program / cross-system analysis
- Used by others:
  - J2/J6 for supportability certifications (CJCSI 6212 & CJCSI 3212)
  - Service Uses such as Gap Analysis
  - Testing community (JITC Interoperability Certification)
  - Joint Spectrum Center review and IA status
  - Study groups (e.g., Joint Forces Interoperability Review Team, Welch Panel, & Joint System Engineering Review Team)
  - Net-Centric Assessments

# ISP Process




JCPAT = Joint C4I Program Assessment Tool
JMAAT= Joint Mission Area Analysis Tool

# ISP Relationship to DoD 5000 Acquisition Process




*** DoD 4630 extends requirements**

**** Program Init. may precede MS B**

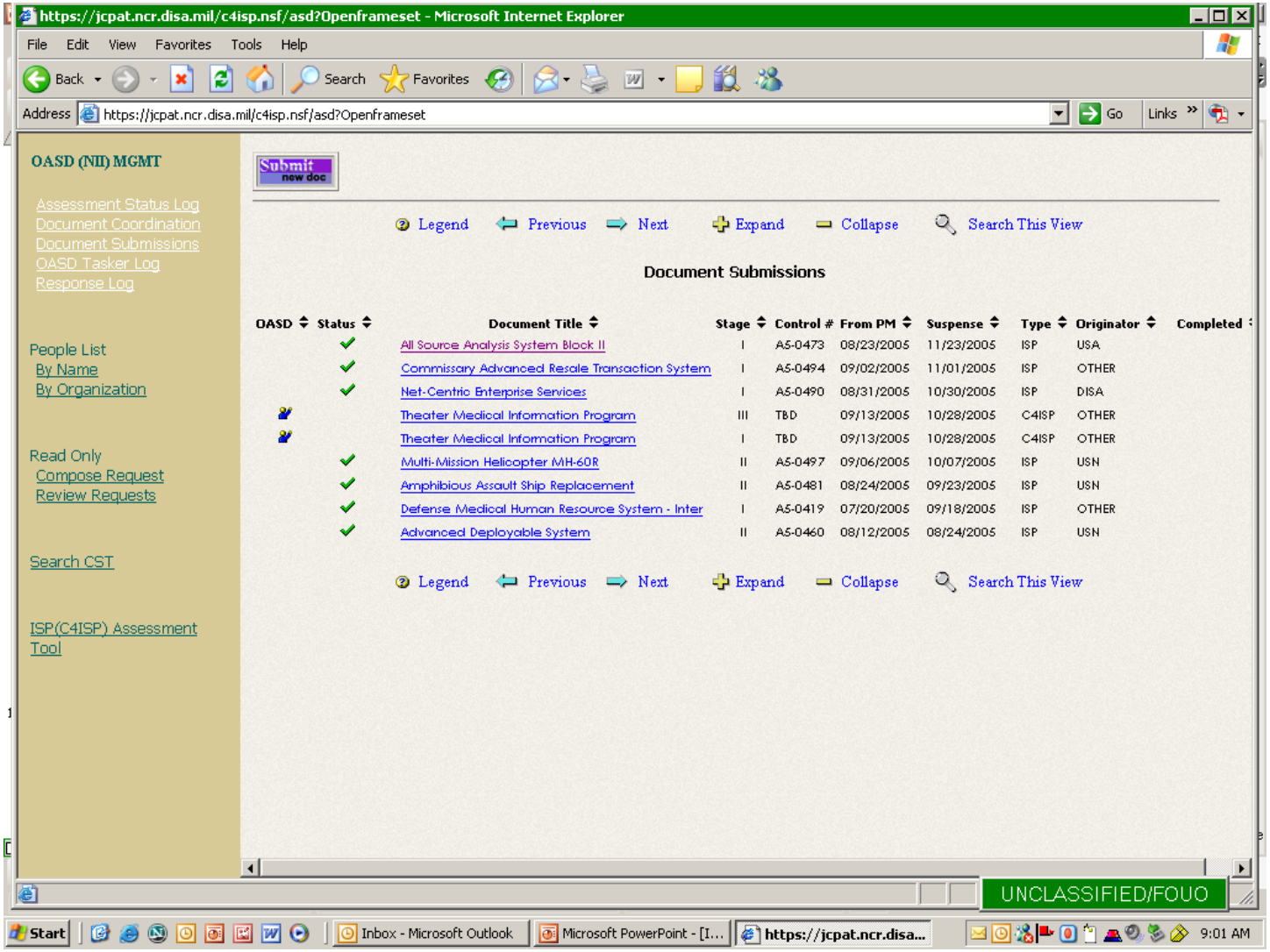
**The Number of reviews of a particular program v**
**Space Programs see NS Policy 03-01**

# JCPAT-E Tool


https://jcpat.ncr.disa.mil/jecoweb.nsf/c4isp?OpenPage - Microsoft In
UNCLASSIFIED\FOUO
File Edit View Favorites Tools Help
Back Search Favorites
Address https://jcpat.ncr.disa.mil/jecoweb.nsf/c4isp?OpenPage
Go Links
ATTENTION!
Announcements:
Please be advised the tool navigators have been upgraded to adhere to Section 508 standards.
For additional Section 508 standards information refer to http://www.section508.gov
The Office of the Assistant Secretary of Defense, Networks and Information Integration (OASD (NII)) is required by DoD Interim Defense Acquisition Guidebook to review all C4ISP documents for ACAT I and IA programs, and for other programs in which OASD(NII) has indicated a special interest. This review is performed on the ISP(C4ISP) Assessment Tool in the JCPAT Tool suite. The ISP(C4ISP) Assessment Tool provides paperless, web-based support for ISP and/or C4ISP document submission, assessor review and comment submission, collaborative workspace, and consolidated review comment rollup. The DISA JCPAT Tool Functional Analyst is available to assist users with ISP(C4ISP) Assessment Tool functionality and to establish tool user accounts. A repository of previous and current ISP/C4ISP documents is available for viewing in the ISP(C4ISP) Assessment Tool Document Repository. The governing document for C4ISPs is DoDI 5000.2 with additional guidance information provided in the Interim Defense Acquisition Guidebook.
DOD aquisition documents are available at http://deskbook.dau.mil.
program manager
isp (c4isp) management
assessors/reviewers
read only
document repository
jcpat main page
mission statement
user's manual
change password
request account
pocs
ISP (C4ISP) Assessment Tool
photo credits
version 3.0
Done
Internet
Start
Inbox - Microsoft Outlook
ISP_TRAINING_NOV2004...
https://jcpat.ncr.disa....
2:33 PM

# JCPAT-E Tool

**Continued**



# ISP Content

| C4ISP | | ISP |
|---|---|---|
| Chapter 1: INTRODUCTION | Provides an introduction and acquisition s | Chapter 1: Program Information |
| Chapter 2: SYSTEM DESCRIPTION | Identifies high-level information about the system being acquired | |
| Chapter 3: OPERATIONAL EMPLOYMENT | Identifies operational and architectural information | |
| Chapter 4: DERIVED C4I SUPPORT REQUIREMENTS | Provides analysis and analysis results that C4ISR and IT/NSS support requirements | Chapter 2: Analysis |
| Chapter 5: POTENTIAL C4I SHORTFALLS & PROPOSED SOLUTIONS | Identifies shortfalls in available or projecte C4I support and interoperability | Chapter 3: Issues |

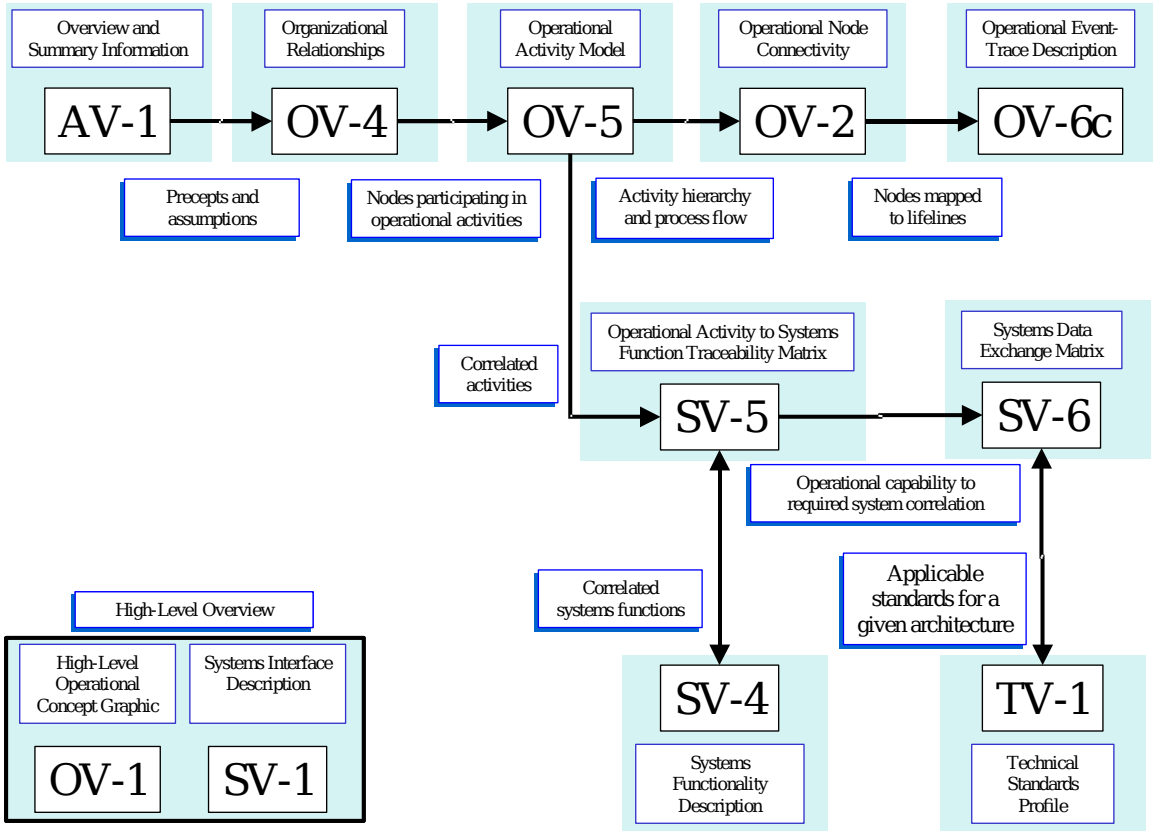
- Note: Supporting appendices provide amplifying data

- Note: Supporting appendices provide amplifying data and Additional architecture views

# ISP Analysis Steps

| |
|---|
| **Step 1:** Identify the warfighting missions (or functions within the enterprise business domains) |
| **Step 2:** Identify information needed to support operational/ functional capabilities for each warfighting mission identified in step 1 |
| **Step 3:** Determine the operational users and notional suppliers of the information needed |
| **Step 4:** Establish the quality of the data needed to support the functions identified in the programs integrated architecture. |
| **Step 5:** Determine if timeliness criteria exist for the information. |
| **Step 6:** Determine / Estimate the quantity of information of each type that is needed. |
| **Step 7:** Discuss how the information will be accessed or discovered. |
| **Step 8.** Assess the ability of supporting systems to supply the necessary information. |
| **Step 9.** Discuss RF Spectrum needs. |
| **Step 10.** Perform a Net-Centric Assessment. (Network-Centric Checklist) |
| **Step 11** Discuss the program's inconsistencies with the GIG Integrated Architecture and its strategy for getting into alignment. |
| **Step 12.** Discuss the program's Information Assurance strategy and reference the Program Protection Plan. |
| **Step 13.** Identify Information support needs to support development, testing and training. |

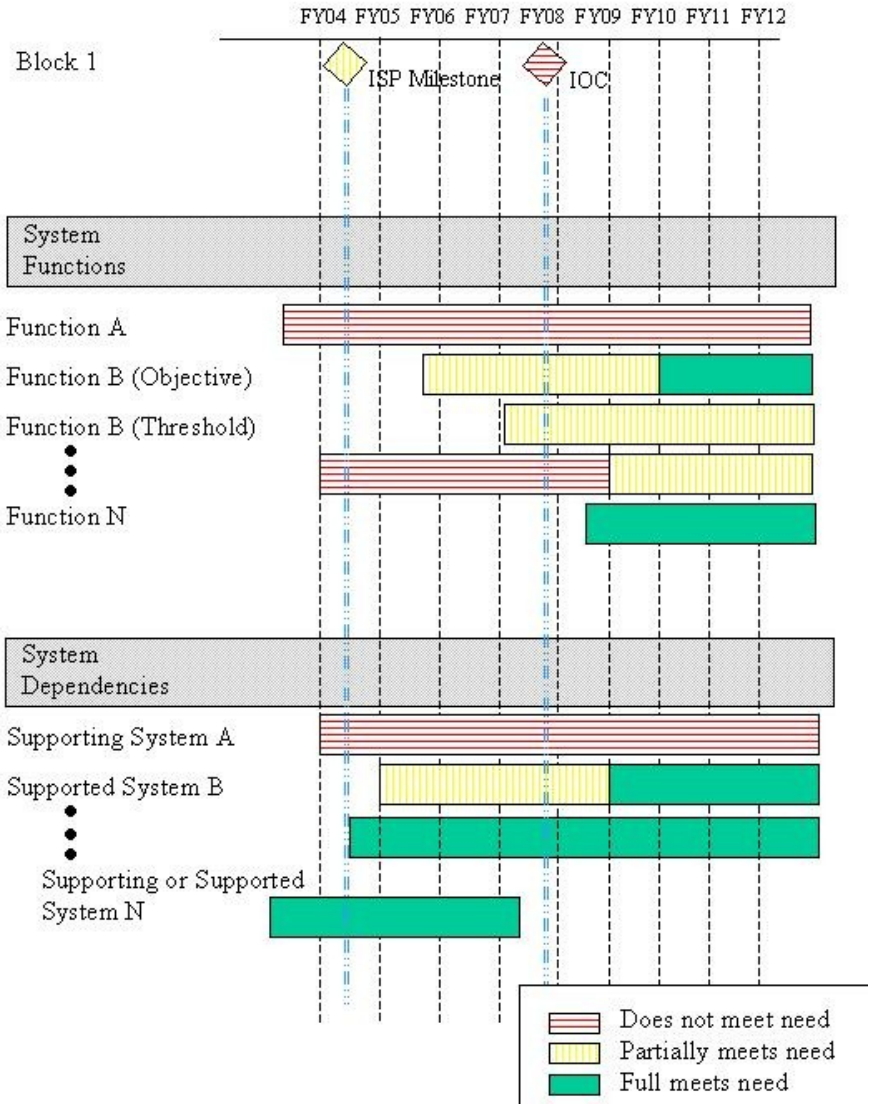
# ISP Architecture Views



# ISP Architecture Analysis

| Architectural View | Area For Analysis | | | | | |
|---|---|---|---|---|---|---|
| | Overview | Information Need/Dependency | Information Quality | Information Quantity | Information Sources | Information Timeliness |
| AV-1 | ● | | | | | |
| OV-1 | ● | | | | | |
| OV-2 | | ● | | | ● | |
| OV-4 | | ● | | | | |
| OV-5 | | ● | | | | ● |
| OV-6c | | ● | | | | ● |
| SV-1 | ● | ● | | | ● | |
| SV-4 | ● | ● | | | | |
| SV-5 | | ● | ● | ● | ● | ● |
| SV-6 | | ● | ● | ● | ● | ● |
| TV-1 | | ● | ● | | | ● |

# ISP Dependency Analysis



# ISP Analysis Considerations

- Signature data
- Levels of specificity
- Specific data format
  - Format of location data
- CEP or Linear EP

# ISP Analysis Considerations
Continued

- Targeting Support
- Geospatial Information
- Mission Planning
- Intelligence Quality / Quantity
  - IMINT
  - SIGINT
  - MASINT
- Computer Resources

# ISP Analysis Considerations

Continued

- Transport mechanism (Radio, Satellite, Relay, etc.)
- Networks details (TCP/IP, sub-nets) -- in place (current) and

  future (LAN, WAN, CENTRIX)
- Frequency, Spectrum, Timeliness, QOS, and Bandwidth
- Databases
- Software Applications
- Critical interfaces
- Connectivity of joint assets
- Data attributes (tagging, form, processing)
- Information assurance

# Issues

| Operational Issues | | | | | |
|---|---|---|---|---|---|
| **Mission** | | | | | |
| **Functional Capabilities impacted** | | | | | |
| **Issue number** | **Supporting system** | **Issue** | **Issue Description** | **Issue Impact** | **Mitigation Strategy/Resolution Path (and Time-Frame)** |
| | | | | | |
| | | | | | |
| **Development Issues** | | | | | |
| | | | | | |
| | | | | | |
| **Testing Issues** | | | | | |
| | | | | | |
| | | | | | |
| **Training Issues** | | | | | |
| | | | | | |
| | | | | | |

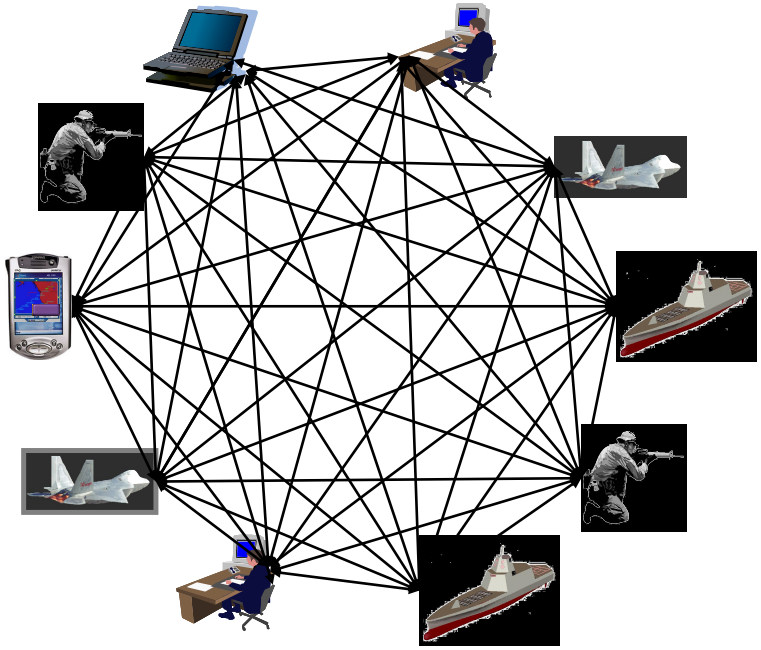
# Net Ready KPP

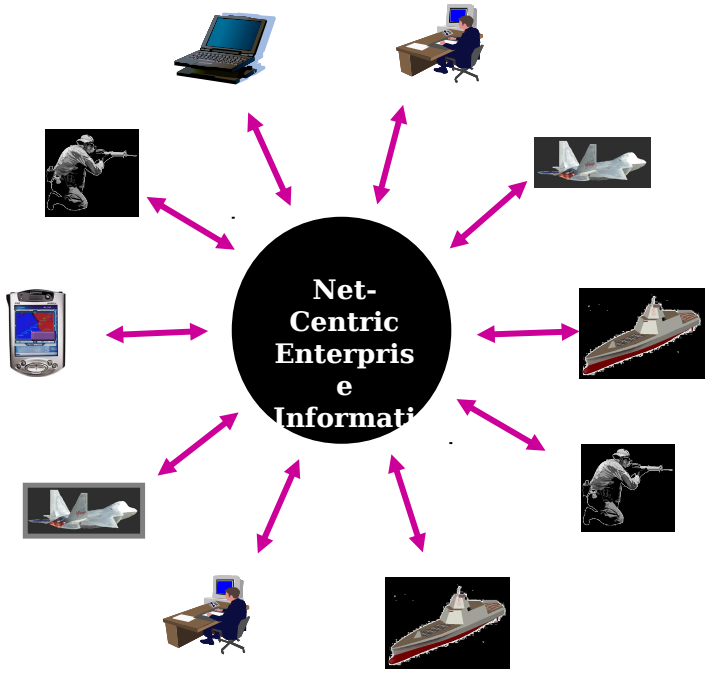
**Four elements of the NR Key Performance Parameters (KPP):**

- Compliance with NCOW Reference Model
- Compliance with GIG KIPs
- Compliance with DoD Information Assurance (IA) Policy
- Required Integrated Architecture Products

# Net Ready KPP Thinking

***Interoperability KPP ---- Net Rea***






**Max number of interfaces = n(n-1), where n = number of systems**

**Max number of interfaces = where n = number of syste**

# Net-Ready Key Performance Parameters (KPP) Parts

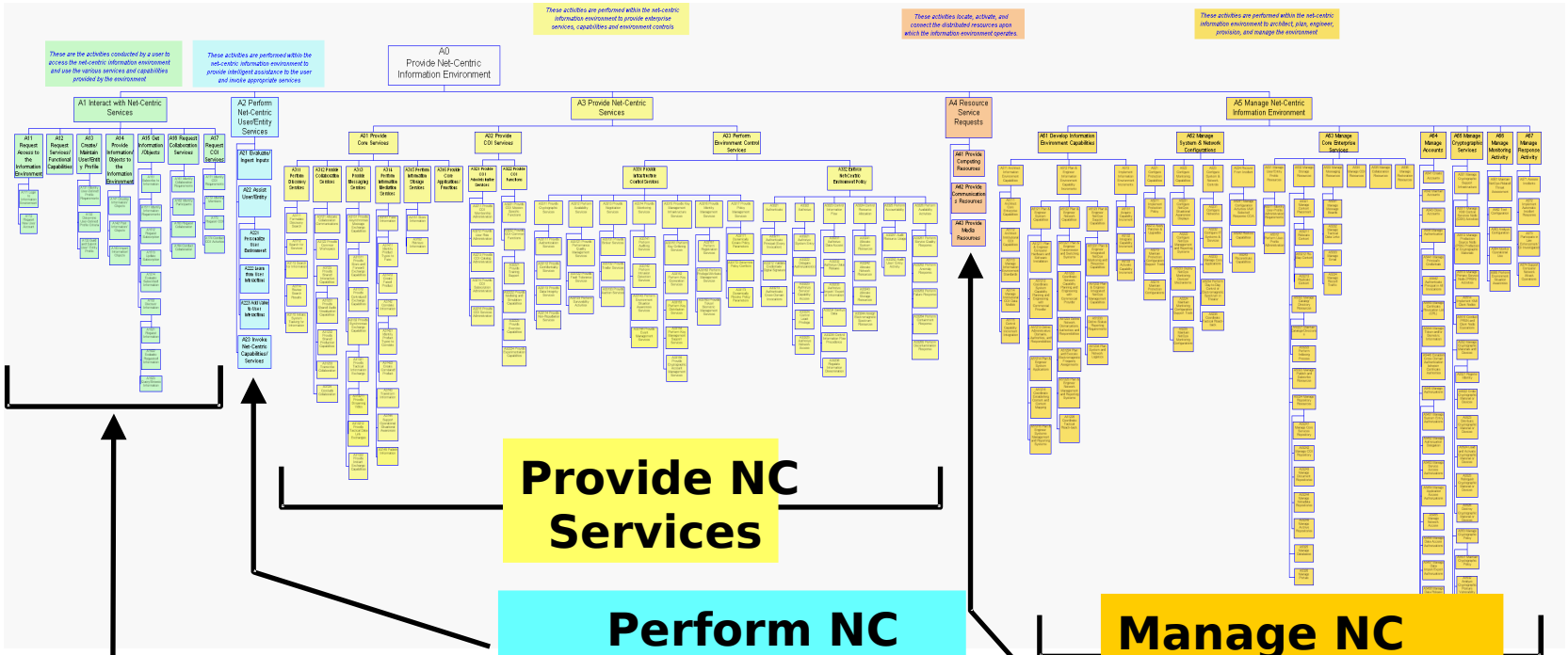
- Net-Centric Operations Warfare (NCOW) Reference Model
- Key Interface Profiles (KIPs)
- Information Assurance (IA)
- Integrated Architecture

- **Net-Centric Operations Warfare (NCOW)**

**Reference Model**

# • Net-Centric Operations Warfare (NCOW)

## Reference ModelContinued



# • Net-Centric Operations Warfare (NCOW)

**Reference Model Continued**

**Program manager compliance with the NCOW RM* is demonstrated through inspection and analysis of a capability's:**

- Use of NCOW RM definitions and vocabulary;
- Incorporation of NCOW RM Operational View capabilities and services in the materiel solution;
- Incorporation of NCOW RM Technical View Information Technology and National Security Systems standards in the technical view products developed for the materiel solution.

* See DAG, Section 7.2.6 for a description of how program managers show compliance with the NCOW RM. In addition, CJCS Instruction 3170.01 and CJCS Instruction 6212.01 for detailed discussions of the inspection and analysis processes

- **Key Interface Profiles (KIPs)**

# • Key Interface Profiles (KIPs)
Continued

## Identify Applicable KIPs

## For those that apply:

- Have applicable Key Interface Profiles definitions been included as part of the KIP compliance declaration (in CDD)?

- Are the information technology standards for each applicable KIP technical view included in the draft TV-1 for the specific Joint integrated architecture (in ISP)?

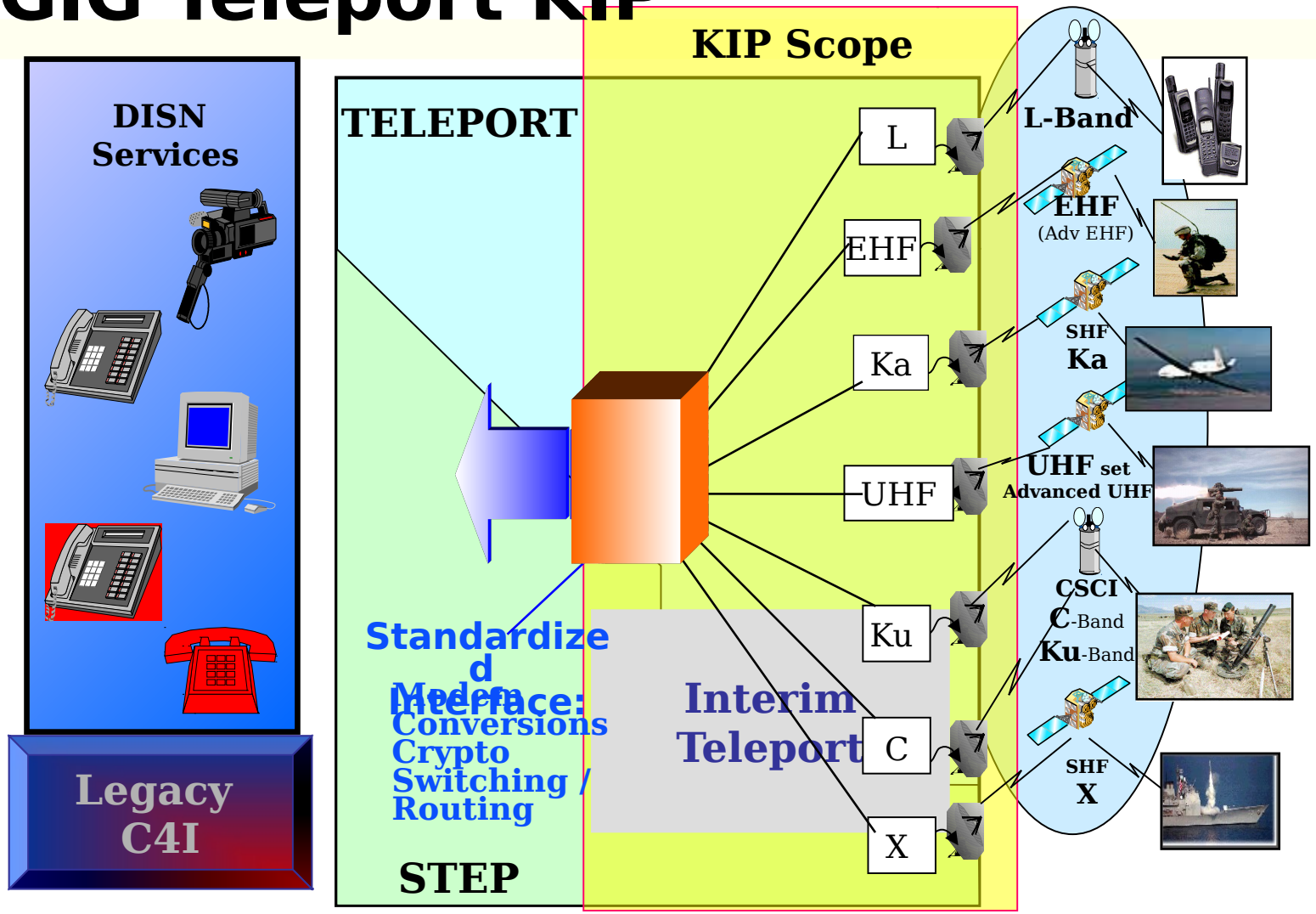
- Are the appropriate KIP test procedures addressed as part of the requirement for interoperability system testing and certification (in TEMP)?

| | ***Communications KIPs*** |
|---|---|
| 1. | Logical Networks to DISN Transport Backbone |
| 2. | Space to Terrestrial Interface |
| 3. | JTF to Coalition |
| 4. | JTF Component to JTF Headquarters |
| 5. | Teleport (i.e., deployed interface to DISN) |
| 6. | Joint Interconnection Service |
| 7. | DISN Service Delivery Node |
| 8. | Secure Enclave Service Delivery Node (e.g., SCI/Collateral KIP) |
| | |
| | ***Computing KIPs*** |
| 9. | Application Server to Database Server |
| 10. | Client to Server |
| 11. | Applications to COE/CCP (NCES/GES) |
| | |
| | ***Network Operations KIPs*** |
| 12. | End System to PKI |
| 13. | Management Systems to (integrated) Management Systems |
| 14. | Management Systems to Managed Systems |
| 15. | IDM to Distribution Infrastructure |
| 16. | Information Servers to IDM Infrastructure |
| | |
| | ***Applications*** |
| 17. | Application Server to Shared Data - FIOP (SADI) |

# • Key Interface Profiles (KIPs)

Continued

## GIG Teleport KIP



- **Information Assurance (IA)**

# • Information Assurance (IA)
**Continued**

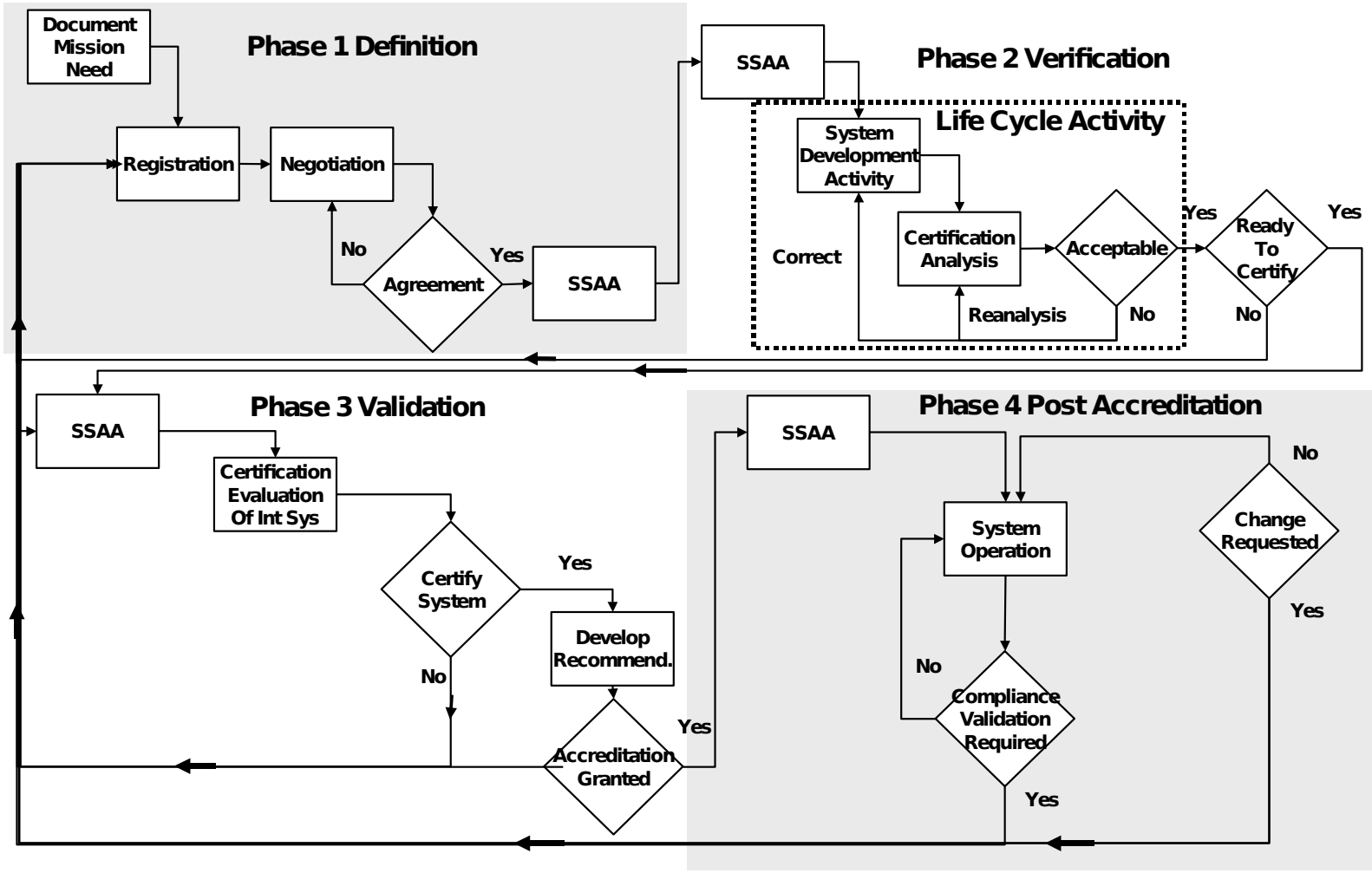
Comply with established accreditation and connection approval processes required for all DoD information systems (DITSCAP*).

- List accreditation documentation (System Security Authorization Agreement – SSAA)
- Identify the Designated Approval Authority (DAA) or DISN DAA
- Reference your Program Protection Plan
- GIG IA Architecture (as appropriate)

* In accordance with DoD Directive 8500.1, all acquisitions of AIS (to include MAIS), outsourced IT-based processes, and platforms or weapon systems with connections to the GIG must be certified and accredited in accordance with DoD Instruction 5200.40, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)* .

# • Information Assurance (IA)

**Continued**




**DITSCAP Process**

- **Integrated Architecture**

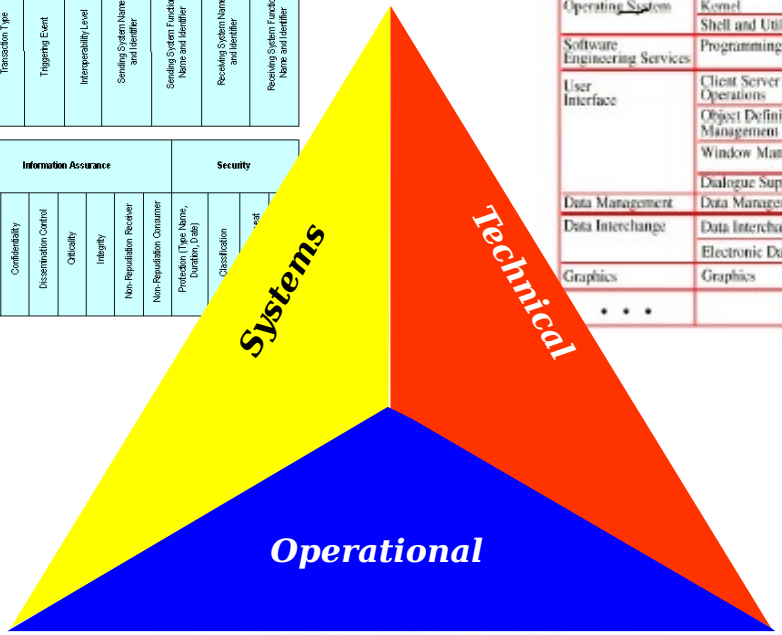
# • Integrated Architecture

**Continued**

| Interface Identification | Data Exchange Identification | Information Description | | | | | | Nature of Transaction | | | Producer | | Consumer | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Systems Interface Name and Identifier | Systems Data Exchange Name and Identifier | Content Description | Format Type | Media Type | Data Standard | Units of Measurement | Accuracy | Transaction Type | Triggering Event | Interoperability Level | Sending System Name and Identifier | Sending System Function Name and Identifier | Receiving System Name and Identifier | Receiving System Function Name and Identifier |

| Interface Identification | Data Exchange Identification | Performance Attributes | | | | Information Assurance | | | | | | | Security | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Systems Interface Name and Identifier | Systems Data Exchange Name and Identifier | Periodicity | Timeliness | Throughput | Size | Access Control | Availability | Confidentiality | Dissemination Control | Orbicality | Integrity | Non-Repudiation Receiver | Non-Repudiation Consumer | Protection (Type Name, Duration, Date) | Classification |

| Service Area | Service | Standard |
|---|---|---|
| Operating System | Kernel | FIPS Pub 151-1 (POSIX.1) |
| | Shell and Utilities | IEEE P1003.2 |
| Software Engineering Services | Programming Languages | FIPS Pub 119 (ADA) |
| User Interface | Client Server Operations | FIPS Pub 158 (X-Window System) |
| | Object Definition and Management | DoD Human Computer Interface Style Guide |
| | Window Management | FIPS Pub 158 (X Window System) |
| | Dialogue Support | Project Standard |
| Data Management | Data Management | FIPS Pub 127-2 (SQL) |
| Data Interchange | Data Interchange | FIPS Pub 152 (SGML) |
| | Electronic Data Interchange | FIPS Pub 161 (EDI) |
| Graphics | Graphics | FIPS Pub 153 (PHIGS) |
| • • • | | |

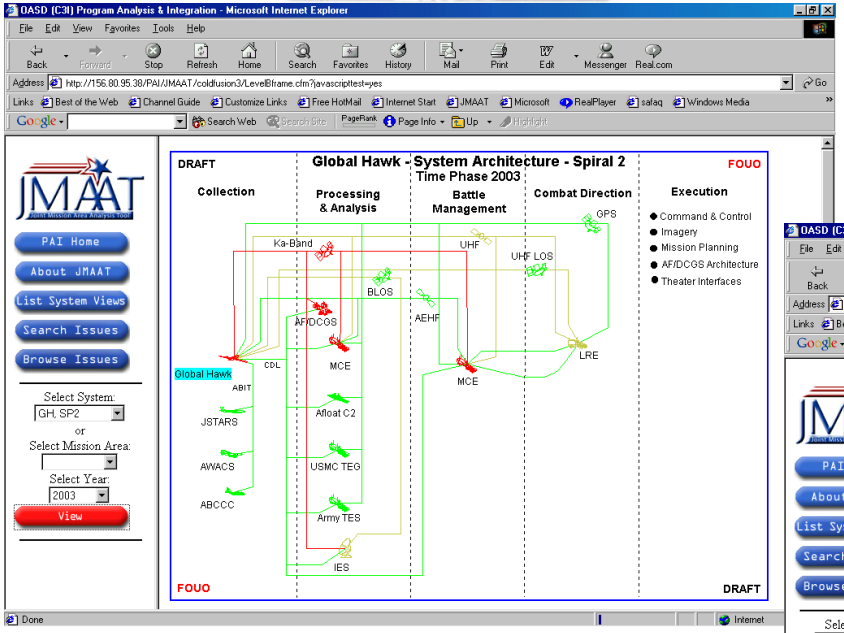


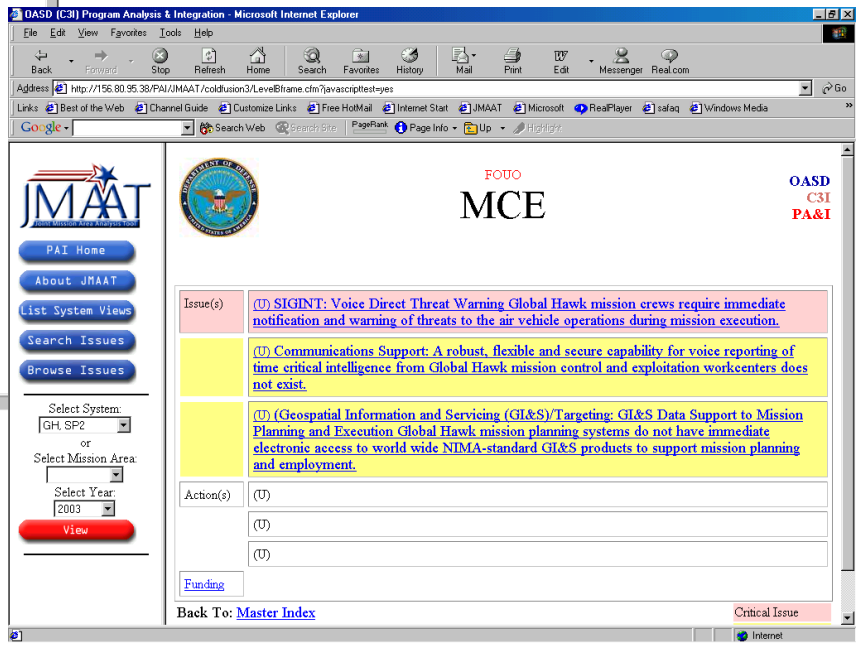


DoD Architecture Framework (DoDAF)

# JMAAT Tool


## Issue Identification and Status



# ISP Pilot Program


OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

NETWORKS AND INFORMATION INTEGRATION

26 August 2005

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, FORCE TRANSFORMATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, JOINT STAFF
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Information Support Plan (ISP) Acquisition Streamlining Pilot Program

The Information Support Plan (ISP) process is defined in Department of Defense (DoD) Instruction 4630.8. The attached Pilot ISP Program will be offered to Program Managers on a voluntary basis effective immediately.

The Pilot Program is designed to improve the ISP process by reducing the number of OSD-level reviews, streamlining the ISP waiver process, and providing a tailored ISP option for ACAT II, III and non-ACAT programs. Program Managers will be encouraged to use this Pilot Program for all future ISPs but may chose to use the existing process in DoD Instruction 4630.8 if they desire. Components should align their ISP processes to accommodate the attached changes.

The Pilot Program is the result of a review under the DoD's Business Initiative Council: AM-45, Streamline the Automated Information System (AIS) Review Process. Will be incorporated into DoD Instruction 4630.8. You comments and recommendations are welcomed during this time-frame. POC for this action is Paul Szabados, (703) 607-0246, paul.szabados@osd.mil.

George Wauer
Director, Architecture and Interoperability

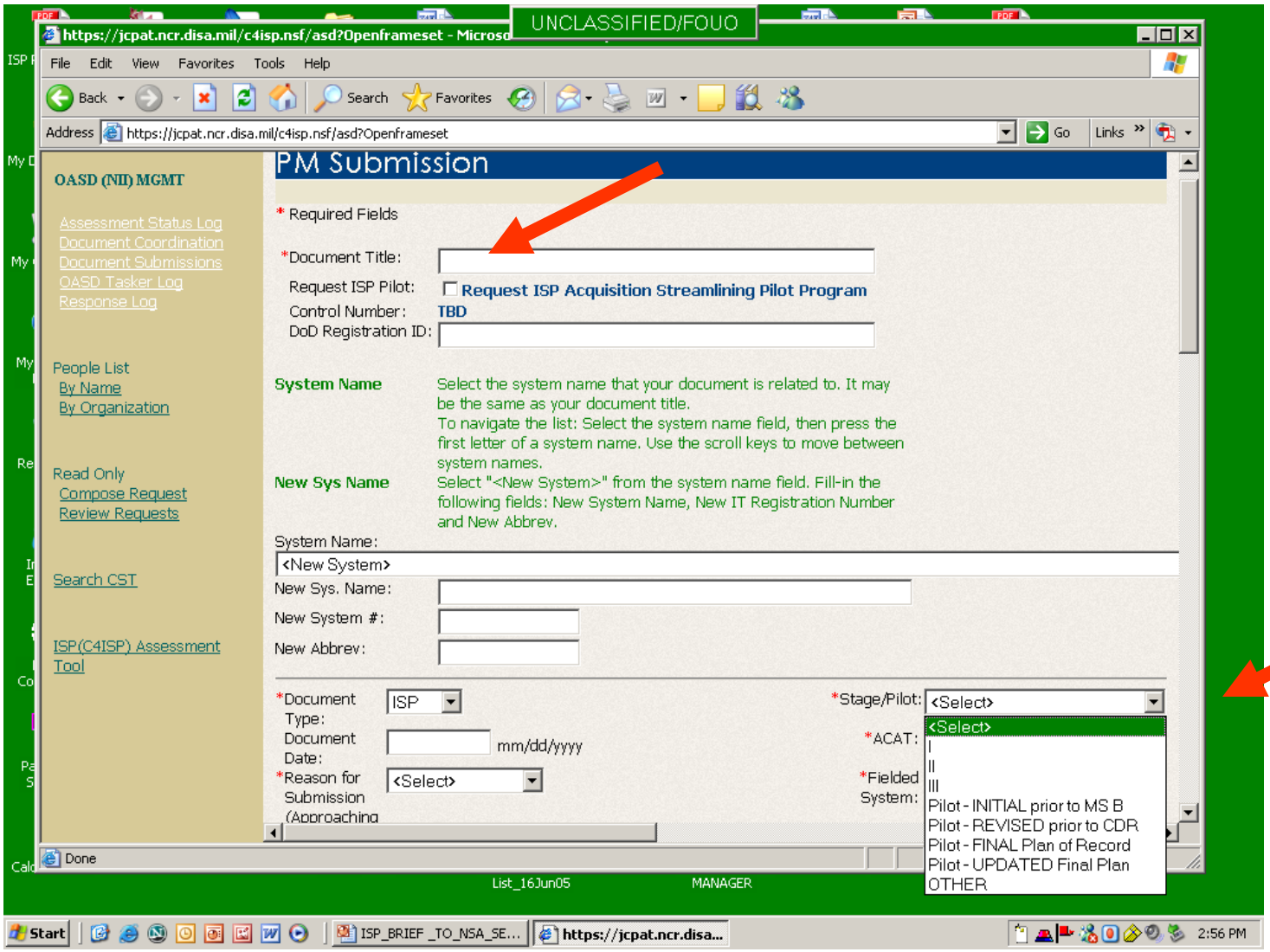
Attachment AS

- Streamlines the review process by requiring a 30 day review at selected points during the acquisition process vice the current three stages of review at each program milestone

- Implements a more efficient ISP waiver process that allows email coordination of the waiver request.

- Eliminates the requirement to enter ISP data into the Acquisition Strategy Report (ASR) and adds a requirement to brief unresolved critical ISP issues at IIPTs / OIPTs for the benefit of the milestone decision authorities.

- Provides a Tailored ISP content and process for lower ACAT and non-ACAT programs.

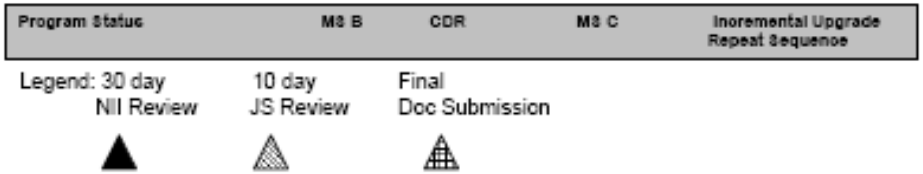

UNCLASSIFIED/FOUO
https://jcpat.ncr.disa.mil/c4isp.nsf/asd?Openframeset - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://jcpat.ncr.disa.mil/c4isp.nsf/asd?Openframeset
Go Links
OASD (NII) MGMT
Assessment Status Log
Document Coordination
Document Submissions
OASD Tasker Log
Response Log
People List
By Name
By Organization
Read Only
Compose Request
Review Requests
Search CST
ISP(C4ISP) Assessment Tool
PM Submission
* Required Fields
*Document Title:
Request ISP Pilot:
Request ISP Acquisition Streamlining Pilot Program
Control Number:
TBD
DoD Registration ID:
System Name
Select the system name that your document is related to. It may be the same as your document title.
To navigate the list: Select the system name field, then press the first letter of a system name. Use the scroll keys to move between system names.
New Sys Name
Select "<New System>" from the system name field. Fill-in the following fields: New System Name, New IT Registration Number and New Abbrev.
System Name:
<New System>
New Sys. Name:
New System #:
New Abbrev:
*Document Type:
ISP
Document Date:
mm/dd/yyyy
*Reason for Submission (Approaching
*Stage/Pilot:
<Select>
<Select>
I
II
III
Pilot - INITIAL prior to MS B
Pilot - REVISED prior to CDR
Pilot - FINAL Plan of Record
Pilot - UPDATED Final Plan
OTHER
*ACAT:
*Fielded System:
Done
List_16Jun05
MANAGER
Start
ISP_BRIEF _TO_NSA_SE...
https://jcpat.ncr.disa...
2:56 PM

- An initial ISP is an ISP version with a review completed prior to MS B; the content emphasizes the functional design and the operational architecture views. The JS (J2/J6) will issue comments on the plan that need to be addressed in the next version.

- A revised ISP is an ISP version with the OSD-level review completed prior to Critical Design Review (CDR) (programs with multiple CDRs should coordinate this submission with ASD(NII)/DoD CIO); the content emphasis is on the system design, system architecture views, and technical architecture views and their relationship to the operational architecture views. The JS (J2/J6) will issue comments on the ISP that need to be addressed in the ISP of record.

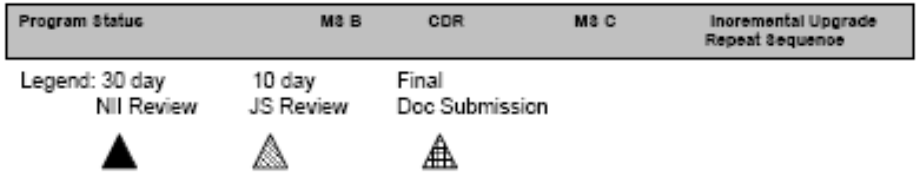
- A final ISP of record is an ISP version with a final acceptance review completed prior to MS C. After the review, an additional 10 day final acceptance review by J2 and J6 is completed prior to MS C. The purpose of this acceptance review will be to issue intelligence and supportability certifications as required in Chairman Joint Chief of Staff Instructions (CJCSIs) 3312.01 and 6212.01D. Upon Joint Staff J2 and J6 certification, the final Component approved ISP will then be submitted to JCPAT-E as the ISP of record.

- An updated ISP can be of two types: (1) an ISP version submitted to update the Final ISP of record which can be submitted to JCPAT-E as the new ISP of record at anytime by the PM and requires no reviews, or (2) an updated ISP version that be provided for the next increment or program upgrade beyond MS C. In this case if there are milestones the ISP will be revised at MS B, CDR and MS C as shown above. If it is a single MS upgrade such as a software revision for an IT system then a single OSD-level review and a JS acceptance review is required.


If the program has no existing C4ISP/ISP and is pre-MS B:


If the program has an existing ISP, Stage I review has been completed, and the program is post-MS B but pre-CDR:


If the program has an existing ISP, Stage II review has been completed, the program is post-CDR, pre-MS C:


If the program has an existing C4ISP/ISP and is post-MS C and the ISP update is associated with an incremental upgrade:


If the program is just updating an existing C4ISP/ISP and the ISP update is not associated with any milestones:


For Tailored ISPs submit to the Joint Staff for review and put the final document into the JCPAT-E ISP repository prior to experimentation conduct or fielding.

3. **ISP Pilot Program Waiver Process.**

The requirement for an ISP may be waived when the JCIDS process or JS J6 analysis has determined that the NR-KPP or I-KPP are not needed; a JCIDS document is not required; or the program does not meet any of the criteria identified in paragraphs 2.2.2, 2.2.3 and 2.2.4 of DoD 4630.8.

Waiver requirements apply to all ACAT and non-ACAT ISPs. Each component shall have an ISP waiver approval process. Waiver requests shall be sent via email to ASD(NII)/DoD CIO by the appropriate component Action Officer for coordination prior to MDA approval. The waiver information will include: the program's name, the next milestone, the capability (ies) the program provides, list any external information and related connectivity, and the rationale for the waiver. ASD(NII)/DoD CIO will respond to the waiver request via e-mail with concur or non-concur. This recommendation will be forwarded to the MDA for final approval.

Upon final approval by the MDA, the Component will provide a copy of the approved waiver package electronically to the ASD(NII)/DoD CIO ISP POCs (see paragraph 8 below).

## 4. ISP Pilot Program Acquisition Strategy and Briefing Requirements.

A summary of the critical ISP issues and resolutions is no longer required to be included in the program's Acquisition Strategy Report. Instead, the Program Manager will be required to brief the critical ISP issues pertaining to IT supportability or inconsistency with DoD IT policy at the MS B and C IIPTs, and, when determined by the IIPT/OIPT, at OIPTs and DABs. Critical issues that strictly deal with ISP document or structure will not be briefed.

ACAT II and below
And Non-ACAT

AV-1
OV-1 (opt)
OV-5
OV-6C (opt)
SV-1 (opt)
SV-5
SV-6
TV-1

5. **ISP Pilot Program Tailored ISP**

ACAT II and below as well as Non-ACAT programs may tailor the content of their ISP upon JS (J6) approval. At a minimum, the tailored plan will provide an explanation of the program's Concept of Operations (CONOPS) and will provide IT supportability analysis of the CONOPS. Additionally, the following set of integrated architecture views is required: an AV-1, OV-1(optional), OV-5, OV-6c (optional), SV-1 (optional), SV-5, SV-6 and TV-1. The program manager will ask the JS (J6) what optional architecture views will be required via email. The JS (J6) will determine if optional views are required. For programs not designated "ISP Special Interest" by ASD(NII)/DoD CIO, the component will obtain from the JS a final decision on the details of the tailored plan subject to the minimums above and any special needs identified by the JS (J2 and J6) for the supportability/interoperability certification processes required by CJCSI 3312.01 and CJCSI 6212.01D. The final Component approved plan will be submitted to ASD(NII)/DoD CIO ISP document repository (via JCPAT-E).

# ISP Review Process

## Current

3 cycles at both MS B and MS C

Stage I: O-6 Level Review (35 days)

Stage II: Flag Level Review (30 days)

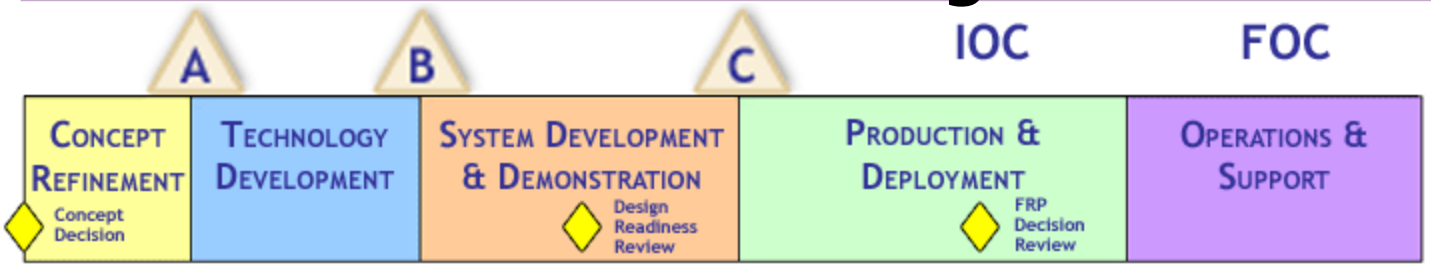
Stage III: Final Plan

## New

Once per milestone cycle

| | |
|---|---|
| MS B (Prog. Init.) | (30 days) |
| Pre-CDR | (30 days) |
| Final Pre-MS C | (10days) |

# ISP Pilot Program




JCIDS Process

Pre-Systems Acquisition

Initial Capabilities Document (ICD)

Capability Development Document (CCD)

Systems Acquisition

Capability Production Document (CPD)

Sustainment

Next Increment

Program Milestones

MS A

MS B

PDR

CDR

MS C

IOC

FRPDR

MS B Next Increment

*ISP Events*

Initial ISP

Revised ISP

ISP of Record

Updated ISP

- Submit Initial ISP
- OSD 30 Day Review
- Comment Adjudication to OSD
- Results feed into PDR
- Posted to OSD JCPAT

- Submit Revised ISP
- OSD 30 Day Review
- Comment Adjudication to OSD
- Results feed into CDR
- Posted to OSD
- JCPAT

- Component Approval
- ISP of record
- Posted to OSD JCPAT

- Submit Revised ISP
- OSD 30 Day review
- Comment Adjudication to OSD

Space Programs Program Milestones

Initial ISP

Revised ISP

ISP of Record

Updated ISP

KDP A

KDP B

KDP C

Final Build Approval

KDP B Next Increment

# ISP Enhancement Project

# Overview

ISP Enhancement Project is an on-going development leading to delivery in Summer 2006.

ISP Version 1.0 is the automated Net-Centric process for producing, reviewing, and leveraging Information Support Plans using XML technology.

The improved process will eventually leverage information from the Net-Centricity Knowledge and Assessment Service (NKAS) for net-centric assessments.

# Objectives

- Improve integration and interoperability of information to support the warfighter and DoD through Net-Centric solutions
- Improve collaboration and information sharing throughout the department on program issues (**searchable and discoverable**) and will improve ability to assess Net-Centric compliance (Streamlined schedule; Improved performance)
- Provide ready access to issues pertaining to IIPTs, OIPTs, Acquisition boards, DAES, JROCs and other associated forum. (Improved performance)
- Benefit DoD by shortening the development cycle of the ISP, while retaining stringent requirements for analysis (Cost savings)
- Allow disparate programs and PMs to **securely** share existing architecture products (Streamlined schedule; Improved performance; Cost savings)
- Allow all PMs to leverage existing architectures into new initiatives (Cost savings)
- Provide a methodology for cross-program analysis and is in compliance with the **Net-Centric Data Strategy** (Improved performance)

# Capabilities

- Developers can post anywhere within security and control constraints
- Only Handle Information Once (NIPRNET/SIPRNET)
- Process is compliant with the Net-Centric Data Strategy
  - Visible, available, usable
  - Tagged
  - Posted to shared spaces
  - Enabling many-to-many exchanges
- Version Control of ISP Documents
  - During development
  - After it is published
- Constraints
  - IA rules
  - Searching NIPRNET for information residing on SIPRNET?

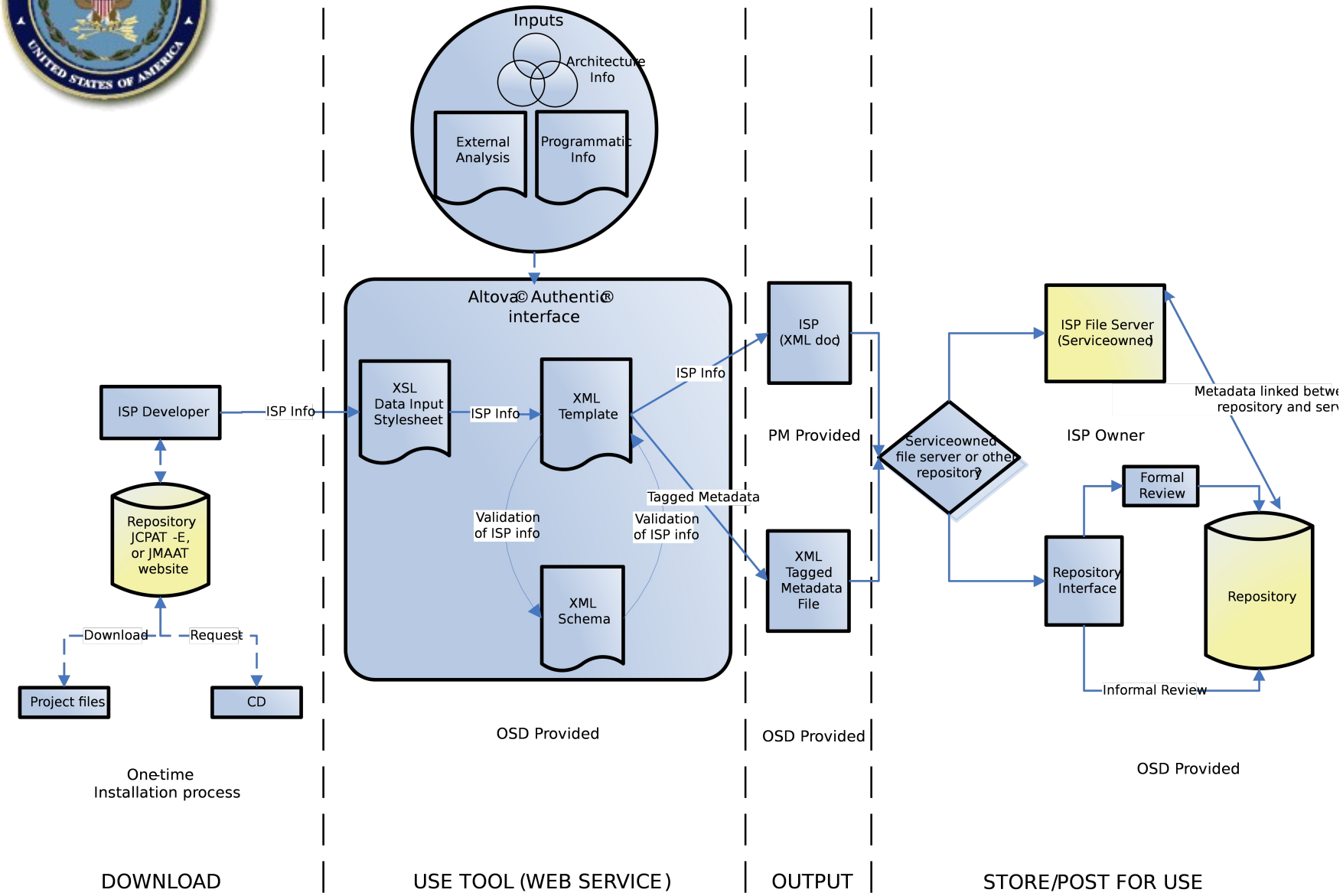
# Stakeholders

- Who are the Stakeholders?
  - ISP developers, ISP reviewers, PMs, PEOs, Agencies and DoD Organizations (Over 200 Users)
  - Sent to over 50 Individual Stakeholders for their review & comments (i.e. The Joint Staff, AT&L, JFCOM, Service Headquarters, Service SYSCOMs, Intelligence Communities,…

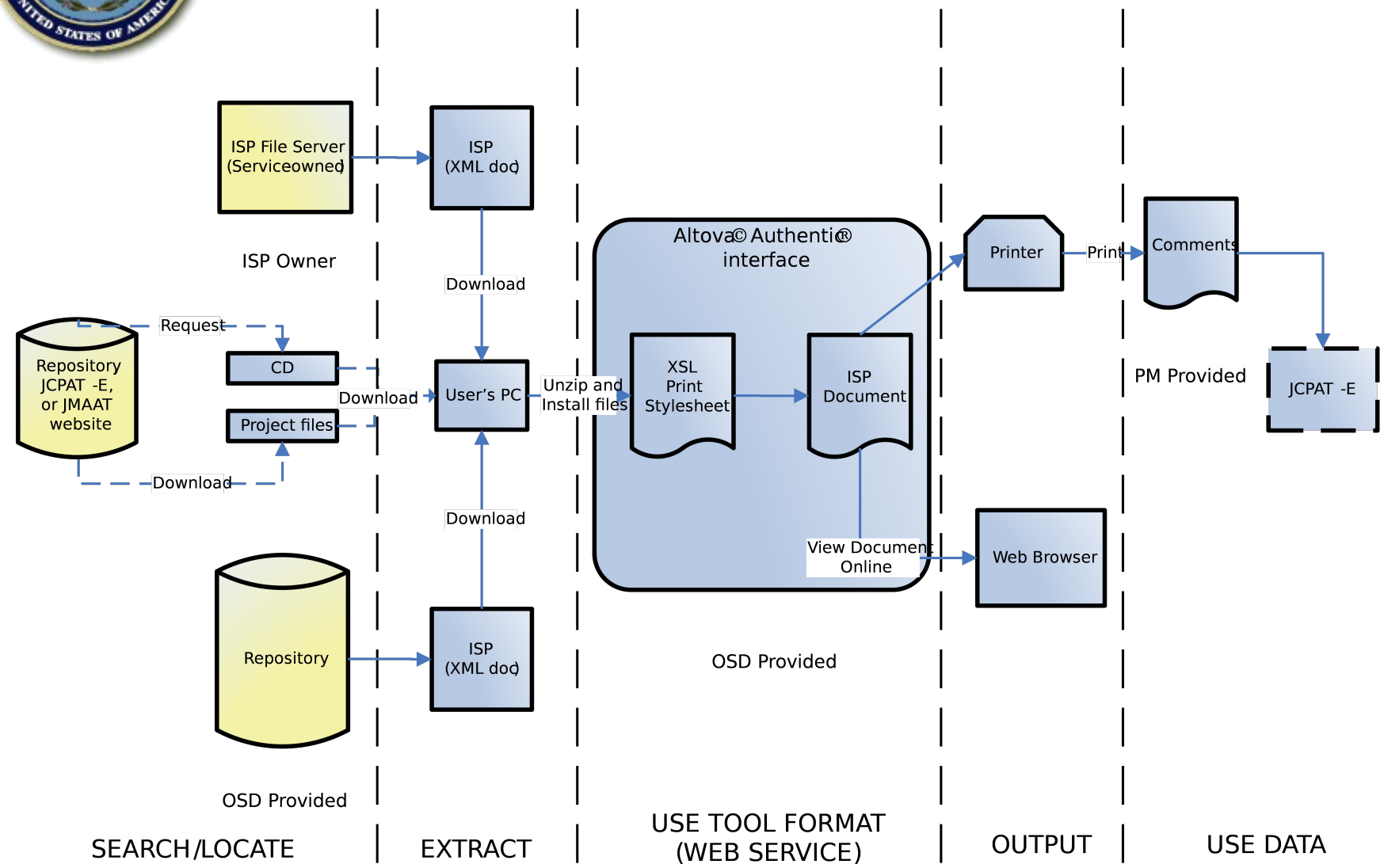
- Comments are being adjudicated by the project team
  - Accepted recommendations will be incorporated into the Vision Document and Requirements Document
  - A Summary of adjudicated comments will be sent to the Stakeholders

- Sample of initial responses
  - Stakeholders have expressed positive support to update the process and supporting system
  - Stakeholders have indicated a need for ISP training
  - Stakeholders are interested in sharing ISP data and artifacts
  - Stakeholders see the ISP project saving time and money

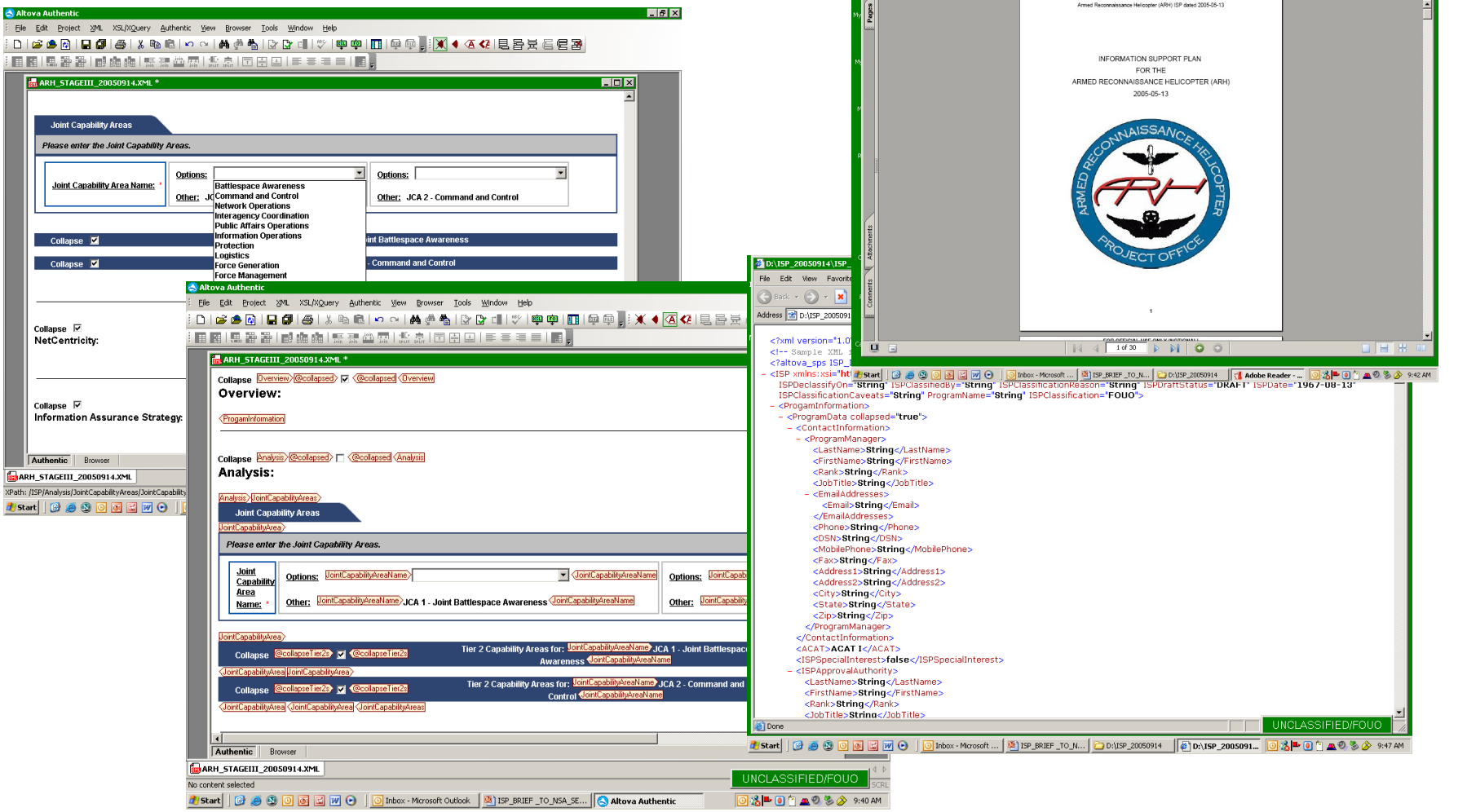
# Input Process



# Output Process

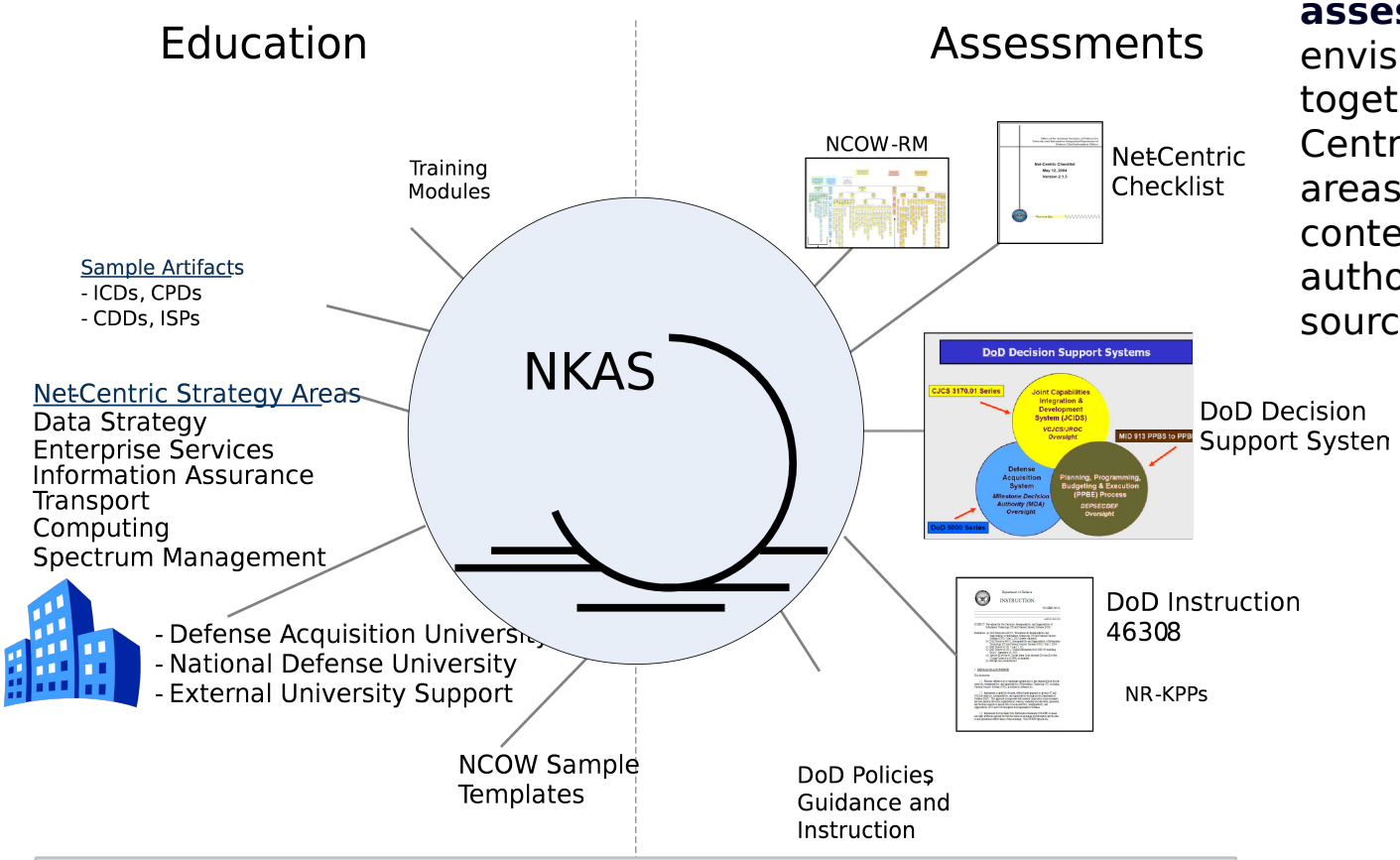


# XML Views


Altova Authentic
ARH_STAGEIII_20050914.XML *
Joint Capability Areas
Please enter the Joint Capability Areas.
Joint Capability Area Name:
Options:
Other:
Battlespace Awareness
Command and Control
Network Operations
Interagency Coordination
Public Affairs Operations
Information Operations
Protection
Logistics
Force Generation
Force Management
Other: JCA 2 - Command and Control
Collapse
NetCentricity:
Information Assurance Strategy:
Authentic
Browser
ARH_STAGEIII_20050914.XML
Overview:
Analysis:
Joint Capability Areas
Other: JCA 1 - Joint Battlespace Awareness
Tier 2 Capability Areas for: JCA 1 - Joint Battlespace Awareness
Tier 2 Capability Areas for: JCA 2 - Command and Control
No content selected
Adobe Reader - [ARH_StageIII_20050914.pdf]
UNCLASSIFIED/FOUO
FOR OFFICIAL USE ONLY (NOTIONAL)
INFORMATION SUPPORT PLAN
FOR THE
ARMED RECONNAISSANCE HELICOPTER (ARH)
2005-05-13
ARMED RECONNAISSANCE HELICOPTER
PROJECT OFFICE
<?xml version="1.0"
<ISP xmlns:xsi="ht
ISPDeclassifyOn="String" ISPClassifiedBy="String" ISPClassificationReason="String" ISPDraftStatus="DRAFT" ISPDate="1967-08-13"
ISPClassificationCaveats="String" ProgramName="String" ISPClassification="FOUO">
<ProgramInformation>
<ProgramData collapsed="true">
<ContactInformation>
<ProgramManager>
<LastName>String</LastName>
<FirstName>String</FirstName>
<Rank>String</Rank>
<JobTitle>String</JobTitle>
<EmailAddresses>
<Email>String</Email>
</EmailAddresses>
<Phone>String</Phone>
<DSN>String</DSN>
<MobilePhone>String</MobilePhone>
<Fax>String</Fax>
<Address1>String</Address1>
<Address2>String</Address2>
<City>String</City>
<State>String</State>
<Zip>String</Zip>
</ProgramManager>
</ContactInformation>
<ACAT>ACAT I</ACAT>
<ISPSpecialInterest>false</ISPSpecialInterest>
<ISPApprovalAuthority>
<LastName>String</LastName>
<FirstName>String</FirstName>
<Rank>String</Rank>
<JobTitle>String</JobTitle>
UNCLASSIFIED/FOUO

# NKAS

A **knowledge and assessment tool** is envisioned to tie together the Net-Centric strategy areas, NCOW-RM content, and other authoritative sources




NKAS Collaboration Service

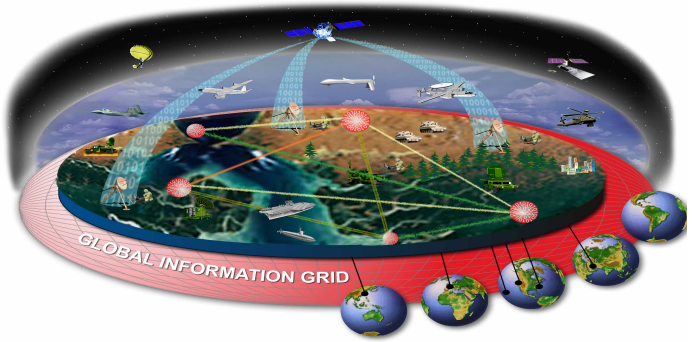
# Remaining Tasks

- Complete Development
- Run Pilot Program
  - Provide CD to PMs, reviewers, ISP developers, and other users
  - Installation help will be available for users
  - Collect feedback and make modifications as required
- Deployment
  - Provide CD to PMs, reviewers, ISP developers, and other potential users
  - Files are available on DOD repositories (JCPAT-E, DARS, etc.)
  - Installation help will be posted for all users
- Policy and Governance recommended changes
  - Defense Acquisition Guidebook DOD 5000.1/DOD 5000.2
  - DODI 4630.8, CJCSI 6212, CJCSI 3170.01D, etc.
  - JCPAT-E and DARS user guides
- Training
  - Embedded training in download package
  - Contractor supported training
- Complete development with any changes following the demonstration

# ISP References and POCs

# DoD Net-Centric Goals

1. ***(Build)*** ***Make information available on a network that people depend on and trust***
2. ***(Populate)*** ***the network with new, dynamic sources of information to defeat the enemy***
3. ***(Protect)*** ***Deny the enemy advantages and expoit weaknesses***




**Net-Centric Attributes**

- **Internet Protocol (IP) Base**
- **Secure and Available**
- **Only Handle Information Once (OHIO)**
- **Smart Pull vice Smart Pus**
- **Data Centric**
- **Quality of Service (QoS)**
- **Application Diversity**
- **Assured Sharing**
- **Ubiquitous Connectivity**

# ISP References

**DoDD 5000.1 and DoDI 5000.2, Operation of the Defense Acquisition System**

**DoD Directive 4630.5 and DoD Instruction 4630.8 Interoperability and Supportability of IT and NSS**

**DoDI 8320.2 Data Sharing in a Net-Centric DoD**

**DoD Net-Centric Data Strategy, May 9,2003**

**Net-Centric Checklist, v 2.1.4, OSD(NII)**

**DAU Acquisition Guidebook**

**JROCM, 236-03, 19 Dec 2003, Policy for Updating Capabilities Documents to Incorporate the Net Ready Key Performance Parameter (NR-KPP)**

**CJCSI 3170.01D, "Joint Capabilities Integration and Development Systems"**

**CJCSI 3312.01**

**CJCSI 6212.01C, 20 November 2003, "Interoperability and Supportability of Information Technology and National Security Systems."**

**National Space Policy 03-01**

**DoD Architecture Framework V1.0**

# ISP Points-of-Contact

**Mr. Paul Szabados (Land, Space, Intelligence) (703) 607-0**
**Mr. Carl Little (Air, PGMs, C2) (703) 607-0**
**Mr. Roger Thorstenson (Maritime and Missile Defense)**
**(703) 607-0506**
**Mr. Bill Barlow (IT Systems) (703) 607-0490**
**Mr. John Feldman (Select Programs) (703) 607-5**

| **Web Sites** | **NIPRNET** | **SIPRNET** |
|---|---|---|
| ***DISA's JCPAT*** | http://jcpat.ncr.disa.mil | http:// jcpat.ncr.disa.smil.mil |
| ***NII's JMAAT*** | | http://www.dsc.osd.smil.mil/pai/inde |
| DAU | http://akss.dau.mil/DAG/ | |
| DSC | http://www.dsc.osd.mil/ | |
| DoD Enterprise Architecture | https://pais.osd.mil/enterprisearchitectures | |

**ISP References available at DSC Website: NIPRNET at http://www.dsc.osd.mil/resources**